В дальнейшем вместо функции x_p и биномиальных коэффициентов мы будем работать с функцией τ_p.

В последующих леммах предполагается, что натуральные числа n, p, q, h, l, v, w удовлетворяют неравенствам

$$q < \frac{1}{2} p^{ln}, \quad v \le w < \frac{1}{2} p^{ln}. \tag{34}$$

Лемма I.I. Пусть

$$b_1 = b_1(v, w) = p^{2(h+ln)-1} + w p^{h+ln} - v, \tag{35}$$

$$d_1 = p^{h+ln} - 1. \tag{36}$$

Тогда число $\tau_p(b_1 - d_1 q, d_1 q)$ лежит в интервале $[0, 2ln]$, если $v \le q \le w$, и в интервале $[h, h+2ln]$ в противном случае.

Доказательство. Рассмотрим три случая: $q < v$, $v \le q \le w$, $w < q$. Ниже $\bar{p} = p-1$, а звездочками заменены неизвестные нам цифры в p-ичной записи чисел $b_1 - d_1 q, d_1 q, b_1$. Стрелки $\leftarrow$ указывают наличие переноса из соответствующего разряда, а символ Δ – отсутствие переноса. Цифры 0, 1, $\bar{p}$ отмечены на основе (35), (36) и соответствующих неравенств, связывающих q с v и w. Основанием для знака $\leftarrow$ является либо наличие в соответствующем разряде у обоих слагаемых цифры $\bar{p}$, либо наличие цифры $\bar{p}$ у одного слагаемого и цифры 0 у суммы, причем во втором случае, очевидно, имел место и перенос из предыдущего разряда. Основанием для знака Δ является наличие в соответствующем разряде у одного из слагаемых цифры 0 и совпадение соответствующей цифры второго слагаемого с цифрой суммы, стоящей в том же разряде. Кроме того, знаком Δ отмечен старший разряд суммы, из которого заведомо нет переноса. Неравенства (34) гарантируют нам, что запись чисел $q, v, w, |q-v|, |q-w|$ имеет длину не более ln. Требуемые неравенства получаются простым подсчетом знаков $\leftarrow$ и Δ.

Случай $q < v$.

$$\begin{array}{rl}
 & \overbrace{}^{h-1}\ \overbrace{}^{ln}\ \overbrace{}^{h}\ \overbrace{}^{ln} \\
b_1 - d_1 q = & 1\,\underbrace{0\ldots0}\ \underbrace{*\ldots*}\ \underbrace{\bar{p}\ldots\bar{p}}\ \underbrace{*\ldots*} \\
d_1 q = & \qquad\quad\ \underbrace{*\ldots*}\ \underbrace{\bar{p}\ldots\bar{p}}\ \underbrace{*\ldots*} \\
\hline
b_1 = & 1\,0\ldots0\ *\ldots*\ \bar{p}\ldots\bar{p}\ *\ldots* \\
 & \Delta\ \Delta\ldots\Delta \qquad\quad \leftarrow\ldots\leftarrow
\end{array}.$$